CLAIMS

1. A countermeasure method against attacks by differential analysis in an electronic component implementing a secret key (K) cryptographic algorithm, the implementation of which comprises a number of successive calculation cycles (T1, ... T16) in order to supply, from first input data (L0, R0) applied to the first cycle (T1), final data (L16, R16) at the output of the last cycle (T16) allowing the production of an encrypted message (C), each calculation cycle using calculation means (TC) for supplying an output data item (S) from an input data item (E), said calculation means comprising the application of a first random value (u) to the input data item (E) and to the output data item (S) in order to obtain at the output an unpredictable data item (S⊕u), characterised in that the method comprises the use of means of applying a second random value (v) to said first input data (L0, R0), according to an EXCLUSIVE OR operation.

2. A countermeasure method according to Claim 1, characterised in that it also comprises the use of means of applying the second random value (v) to the final data supplied by the last cycle (T16), according to an EXCLUSIVE OR operation.

3. A countermeasure method according to either one of the previous claims, characterised in that it comprises, at the end of each cycle, the execution of an additional operation (CP(p(u))) in order to

eliminate said first random value (u) at the output of each cycle.

4. A countermeasure method according to any one of the previous claims, characterised in that it comprises the taking of first and second random values (u, v) and calculation of the calculation means (TC_M) used in each cycle for each new execution of the algorithm.

5. A method according to Claim 4, characterised in that said calculation means (TC_M) are calculated from first calculation means (TC_0) defining, for input data (E), corresponding output data (S), by applying the second random value (v) to said input data ($E \oplus e(v)$) and applying the first random value (u) at least to said output data ($S \oplus u$) of the first calculation means.

6. A countermeasure method according to Claim 5, characterised in that the calculation means (TC_0, TC_M) are constants tables.

7. An electronic security component implementing the countermeasure method against attacks by differential analysis comprising a secret key (K) cryptographic algorithm, the implementation of which comprises a number of successive calculation cycles (T1, ... T16) in order to supply, from first input data (L0, R0) applied to the first cycle (T1), final data (L16, R16) at the output of the last cycle (T16) allowing the production of an encrypted message (C), each calculation cycle using calculation means (TC) for supplying an output data item (S) from an input data item (E), said calculation means comprising the

application of a first random value (u) to the input data item (E) and to the output data item (S) in order to obtain at the output an unpredictable data item (S⊕u), characterised in that first calculation means (TC_0) are fixed in program memory (1) of said component, calculation means (TC_M) used in each cycle being calculated at each new execution of the algorithm and stored in working memory (3), and in that it comprises means (4) of generating first and second random values (u, v) for calculating said calculation means (TC_M).

8. A smart card comprising an electronic security component according to Claim 7.